Risk Assessment

A. Introduction

The Federal Managers' Financial Integrity Act (FMFIA) of 1982, as implemented through OMB Circular A-123, "Management Control Systems," requires Federal managers to perform periodic Risk Assessments. A Risk Assessment is a *brief* evaluation (2–3 hours) of the susceptibility of a component of a programmatic or administrative area to waste, fraud, abuse, or mismanagement. It is a screening device that facilitates rapid identification of potential problems that may require corrective actions.

The purpose of a Risk Assessment is twofold: (1) classifying Management Control Areas (MCAs) into high, medium, and low risk categories (MCAs are the organizational or functional components of an Agency to be evaluated in a Risk Assessment); and (2) scheduling each MCA for further evaluation through the execution of Management Control Reviews (MCRs)/Alternative Management Control Reviews (AMCRs). The schedule of the MCRs/AMCRs will then be reflected in the Management Control Plan (MCP).

Management Controls are operational checks and balances that an organization uses to achieve its specific mission, operational efficiency and effectiveness, compliance with laws and regulations, the safeguarding of resources, and the development of accurate and reliable information.

A Risk Assessment is one phase in a multi-phase review process intended to identify and correct control weaknesses. The overall FMFIA process requires the following steps: organizing the process, segmenting the agency, conducting Risk Assessments, developing MCPs, conducting MCRs/AMCRs, taking corrective actions, tracking Management Control and Corrective Action Plans, and reporting results to the President and Congress.

The underlying principle behind Risk Assessments is that managers should use existing knowledge to self-assess their MCA. This self-assessment concept is an integral part of the FMFIA process. Risk Assessments also facilitate the prompt correction of readily apparent control weaknesses that are amenable to resolution.

In addition, identification of unnecessary controls could result from the Risk Assessment process. Certain control procedures could be identified for elimination or simplification if those controls are found to be irrelevant as a result of program or budget changes, redundant with other controls, or not cost effective or time efficient.

FMFIA and Circular A-123 require Risk Assessments and Management Control Reviews at least once every five years. These enable managers to ensure that there are adequate management controls in place to protect the government resources entrusted to them and to ensure that activities are carried out as intended by their mission. Areas deemed high risk in a Risk Assessment are reviewed first, moderate risk areas next, and low risk areas last. New Risk Assessments should be performed whenever there is a major change or review, e.g., Office of Inspector General (OIG)/General Accounting Office (GAO) review, Congressional inquiry,

identification of a significant problem, etc. The five year Management Control Plan is subject to change depending on results of Risk Assessments.

Most NIH Risk Assessments are carried out on a NIH-wide basis by a team composed of MCA managers, functional managers and other staff who self-assess MCA operations across NIH. Representatives from the intramural, extramural, or administrative communities of NIH with technical and general knowledge of the MCA participate as members of the team in the Risk Assessment process.

The Risk Assessments are performed in six steps starting with preparing for the Risk Assessment meeting, followed by a review of current NIH-wide MCAs or sub-areas to determine if revision is needed, rating sub-areas, determining overall risk for the MCA, documenting and reporting on the Risk Assessment process, and taking subsequent actions.

B. Required Procedures for Conducting Risk Assessment

Step I: Preparing for the Risk Assessment Meeting
The MCA manager has responsibility for assigning the overall risk rating for the NIH-wide MCA and decides what process to use to rate the individual sub-areas. In preparation for this meeting, the MCA manager should identify associated inherent risks, management control objectives, management control techniques, and test checks *for each sub-area*, or entire MCA if there are no sub-areas. The techniques and test checks described should only be those *in place and working*. The manager should also consider how the MCA activities relate to the NIH mission and evaluate the internal control environment of the MCA: (See Appendix 1.)

- *Associated inherent risks* are the actual or potential impact to an MCA if proper management controls are not in place. Inherent risks could include the potential or actual loss of human/animal life, a substantial amount of resources, NIH delegated authorities, adverse impact outside the NIH, programs with a high degree of complexity, or prior review recommendations not implemented. For example, if the motor pool was the MCA being assessed, risks that could be identified are (1) over 100 vehicles could be improperly utilized, (2) inventory value of vehicles is over $2 million, and (3) inventory value of parts/supplies is over $1 million.
- *Management control objectives* are the specific ends to be achieved by management's program activity/administrative function control processes and documents. For example, if the motor pool was the MCA being assessed, objectives that could be identified are (1) to prevent the unauthorized use of motor vehicles, (2) to prevent theft of vehicles, and 3) to prevent loss of parts/supplies.
- *Management control techniques* are the management control processes and documents used within each sub-area. Examples of control techniques that could be used in the motor pool are (1) keys are kept in secure area and released with a trip ticket properly authorized, (2) vehicles are kept in a secure area, and (3) inventory is kept secure with a record of parts/supplies and the mechanic who uses them.
- *Test checks* are all the existing methods of determining whether management control techniques are working in accordance with management control objectives for the MCA. Examples of test checks that could be used in the motor pool are (1) audit trip tickets and

confirm mileage on car odometers, (2) ongoing audit of the status and location of all vehicles, and (3) audit inventory of parts/supplies.

The MCA manager should distribute to the team members, prior to the meeting, the associated inherent risks, objectives, controls and test checks currently in place and working (See Appendix 1.); previous reviews or audits of the MCA in the last five years; audits of other agencies within the last five years, especially those citing any weaknesses that may be related to NIH; prior MCRs/AMCRs and Risk Assessments; and the current segmentation of the MCA. The inability to complete all information on Appendix 1 is probably an indication that a weakness exists. All of this information should be used to assist in determining the appropriate risk level for each sub-area.

The NIH-wide Risk Assessment team should be made up of high level managers that includes the MCA manager, functional area managers, OD functional managers, and ICD representatives with technical and general knowledge of the MCA. Selection of the Risk Assessment team members is the responsibility of the MCA manager.

Step II: Perform Preliminary Assessment/Revision of Current MCAs/Sub-Areas
Based on the information (identified in Step I) distributed by the MCA manager, the Risk Assessment team reviews current MCAs and sub-areas to determine if the areas identified in the current MCP should be modified. If current MCAs or sub-areas are deleted, added, or changed, Management Review Board (MRB) approval is required. However, the rating process can and should proceed in the same meeting so as to expedite the rating process. Any modifications to the MCP should be submitted as part of the Risk Assessment to the Office of Management Assessment (OMA) for subsequent approval by the MRB.

Step III: Rating Sub-Areas (or Overall MCA if there are no Sub-areas)

a. Risk Assessment Meeting(s)

To rate the individual sub-areas for each MCA, or overall MCA if there are no sub-areas, the MCA manager convenes one or more meeting(s) attended by the Risk Assessment team members. The meeting should be structured to facilitate determination of risk ratings and preparation of the attached "Report of Risk Assessment" form. The number of meetings required is determined based on the number, scope, and complexity of the sub-areas under each MCA. An overall risk rating of the MCA should be derived from the sub-area ratings as described in Step IV. All Risk Assessment meetings must be attended by OD functional managers and ICD representatives with technical and general knowledge of the NIH-wide MCA.

b. "Risk Assessment Rating of Sub-Area" form

The attached "Risk Assessment Rating of Sub-Area" form contains fourteen questions to be answered “yes” or “no.” The MCA manager should supply documentation on all management controls in place and tests used to determine compliance. Each of the questions should be answered by obtaining input from the Risk Assessment team, for each of the sub-areas within the MCA or overall MCA if there are no sub-areas. *A risk rating should be determined for*

each sub-area, and an overall MCA rating should be derived from individual ratings. Make as many copies of the "Risk Assessment Rating of Sub-Area" form as necessary to rate each sub-area.

There are six categories of risk factors addressed in this questionnaire: General Control Environment, Inherent Risk, Existing Safeguards, Automated Information Systems, Financial Management, and Other Considerations. The questionnaire combines all of these into two categories, General Control Environment and Inherent Risk. Questions relating to all of the other risk factor categories are incorporated into these two categories.

c. Criteria about Controls In Place

The following criteria about the controls in place should be considered when answering the Risk Assessment questions:

•Do controls provide full coverage of the appropriate areas?
•Do the controls provide "reasonable" assurance that the objectives are being met?
•Are the controls cost effective and time efficient?
•Are the controls adjusted for program or budget changes?
•Are the controls documented?

d. Determining Sub-Area Ratings

The risk in a sub-area is rated by counting the number of "no" answers to the fourteen questions on the "Risk Assessment Rating of Sub-Area" form as follows:

2 or less	No	=	Low Risk
3–4	No	=	Medium Risk
5 or more	No	=	High Risk

Some of the questions refer to high risk areas and are so noted. A "no" to any of these high risk items *automatically* puts the sub-area (or the MCA, if there are no sub-areas) into a high risk category.

A "no" response to any question requires immediate corrective action by the functional manager to resolve the problem. There is no need to wait for a formal review. A corrective action plan addressing each "no" shall be submitted to the OMA within 30 days of the signed Risk Assessment. (See Appendix 2.)

Step IV: Determining an Overall Risk Rating for the MCA—Guidelines

After each of the sub-areas is rated (or MCA if there are no sub-areas), an overall risk should be established for the entire MCA. This overall rating is assigned based on the *percentage* of sub-areas rated as *high risk*. As a guide, this can be done by (1) counting the number of sub-areas with high, medium, and low risk ratings (2) calculating the percentage of sub-areas rated as high risk and (3) using the chart below to assign an overall rating.

% of Sub-Areas High Risk	MCA Rating
Under 25% 25–49% Over 49%	Low* Medium High
**Except if the majority of sub-areas are rated as medium, then a "medium" MCA rating should be assigned rather than a "low" rating.*	

For example, the sub-area ratings for a given MCA are as follows:
High, Low, High, Medium, Low, Low
(1) # of High = 2, # of Medium = 1, # of Low = 3
(2) 2/6 = 33%
(3) The MCA Rating = Medium

If there are no sub-areas rated as high risk, the MCA should be rated either medium or low based on which of these ratings has the higher percentage. If the ratings in the sub-areas are equally distributed between medium and low, then the MCA rating should be a medium.

These are *general guidelines* for assessing the overall risk for a MCA. If you have major weaknesses in one or two sub-areas which are particularly sensitive, significant, or visible, you may decide to rate the overall MCA as high risk.

Step V: Documenting and Reporting on the Risk Assessment Process
A record must be kept using the "Report of Risk Assessment" form, of the outside attendees of the Risk Assessment meetings. Further, the MCA manager and all sub-area managers must sign the completed "Report of Risk Assessment" form. Records must be kept by the MCA manager for five years, or until the next Risk Assessment.

Step VI: Subsequent Actions After the Risk Assessment is Performed
Once the Risk Assessment is completed, it is necessary to indicate what type of review will be done, either a MCR and/or an AMCR. This must be recorded on the "Report of Risk Assessment" form. The preferred process is to have only one review for each MCA. However, both a MCR and an AMCR may be required in some areas because neither of the planned individual reviews would cover all administrative and programmatic aspects. For example in DFM, a CFO Audit is used to review the Service and Supply Fund and the Management Fund; and a MCR is used to review other MCAs.)

A MCR is a detailed evaluation or examination of a program or administrative activity to determine whether necessary controls are in place and producing the intended results: to avoid mismanagement, unauthorized use of resources, erroneous reports or data, illegal or unethical acts, or adverse or unfavorable public opinion.

An AMCR is a review that accomplishes the same objectives as that of a MCR in a less labor-intensive manner. AMCRs make use of recently issued audits of a MCA's major control systems performed by the IG or GAO, as well as management evaluations and outside certifications that are utilized in existing management reporting and review processes. An AMCR can be carried out instead of a MCR if all of the objectives of a MCR are accomplished and testing is performed. The Department and NIH encourages maximum usage of AMCRs.

In addition to performing a MCR or AMCR, subsequent actions to a Risk Assessment may also include taking immediate corrective action where warranted, such as conducting preliminary reviews focused on areas of concern, requesting an audit, establishing monitoring procedures, developing and implementing staff training programs, issuing clarifying instructions, or modifying procedures or documents. If a MCA is identified as high or moderate risk because of a control weakness that is amenable to resolution, prompt corrective action must be taken to correct the control weakness.

Corrective Action Plans

Time-phase Corrective Action Plans (CAPs) are required for *every* weakness and risk noted during Risk Assessments and MCRs/AMCRs. This plan should identify the MCA, describe the weakness, outline the consequences, detail the course of action to correct the weakness, and estimate the time frame for fully correcting the weakness. (See Appendix 2.) *Several non-material weaknesses can be combined into one CAP.* If Material weaknesses also exist, they should be included on a separate plan. The CAPs should be submitted to OMA within 30 days of the signed Risk Assessment.

C. Risk Assessment Package

Completed Risk Assessment Packages must include the following materials:

- Any modifications to the MCP.
- "Report of Risk Assessment" form.
- "Risk Assessment Rating of Sub-Area" form for each sub-area or overall MCA, if there are no sub-areas.
- "Documentation for Risk Assessment and Management Control Review" for each sub-area or MCA as appropriate (Appendix 1).
- Corrective Action Plans (within 30 days) for any problem areas (Appendix 2).

D. Questions about the Process

If you have any questions about performing a Risk Assessment, please contact OMA (496-2461).